BY ORDER OF THE COMMANDER
AIR FORCE SPACE COMMAND

AIR FORCE SPACE COMMAND
INSPECTION CHECKLIST 31-25

1 MAY 2003

Security

SECURITY FORCES MANAGEMENT INFORMATION SYSTEM (SFMIS) (WING)

NOTICE: This publication is available digitally on the AFDPO WWW site at: **http://www.e-publishing.af.mil.**

OPR: SFOP (SMSgt Charles J. Smith)

Certified by: SF (Col Michael W. Hazen)
Pages: 3
Distribution: F

This checklist reflects Command requirements for the Security Forces Management System (SFMIS) program to prepare for and conduct internal reviews.

1. References have been provided for each item. Critical items have been kept to a minimum and are required by law, executive orders, DoD Directives, or safety guidelines; which, if not complied with, could result in significant legal liabilities, penalties or mission impact. The IG will inspect all critical items on AFSPC checklist. In addition, the IG will work with the functional staff prior to a major inspection to identify non-critical items that should be inspected at a particular unit.

2. This publication establishes a baseline checklist. The checklist will also be used by the Command IG during applicable assessments. Use the checklist as a guide only. AFSPC Checklists will not be supplemented. Units may produce their own standalone checklists as needed to ensure an effective and thorough review of the SFMIS program. Units are encouraged to contact the Command Functional OPR of this checklist to recommend additions and changes deemed necessary. See Attachment 1.

WILLIAM L. SHELTON, Brig Gen, USAF
Director of Air and Space Operations

ATTACHMENT 1

SECURITY FORCES MANAGEMENT INFORMATION SYSTEM (SFMIS) PROGRAM (WING)

Table A1.1. Checklist.

SECTION 1: SECURITY FORCES MANAGEMENT INFORMATION SYSTEM (SFMIS) PROGRAM (WING)MISSION STATEMENT: To ensure effective management of the Security Forces Management Information System (SFMIS) program. All references are from AFI 31-203, ***Security Forces Management Information System (SFMIS),*** unless otherwise stated.			
1.1 CRITICAL ITEMS:	**YES**	**NO**	**N/A**
1.1.1. Has the unit developed procedures to meet the congressionally mandated Defense Incident Based Reporting System (DIBRS) requirement? (Para 1.1.1.)			
1.1.2. Does the unit report criminal activity as outlined in para 1.2.3.? (Para 1.2.4.)			
1.1.3. Has the unit commander appointed a System Administrator (SA)? (Para 1.2.7.1.)			
1.1.4. Does the SA grant permission and access for personnel requiring access to SFMIS in the performance of official duty? (Para 1.2.7.1.)			
1.1.5. Does the SA ensure all incidents identified under DIBRS reporting criteria are reported through SFMIS? (Para 1.2.7.3.)			
1.1.6. On the first day of each month, does the unit accomplish a monthly computer run of the previous month's criminal summary report? Is the report compared with the local AFOSI's Defense Clearance and Investigation Index (DCII) reporting criteria to ensure all pertinent criminal activity is reported? (IC 2001-1 to AFI 31-203, para 1.2.7.4.)			
1.1.7. Has the installation security forces commander ensured all reportable DIBRS incidents, identified in DoD 7730.47-M are accomplished using AF Form 3545, Incident Report? (IC 2001-1 to AFI 31-203, para 2.1.4.)			
1.1.8. Is the AF Form 3545 completed in such a way to capture the necessary data reportable to the DMDC? (Para 2.1.4.)			

1.2. NON-CRITICAL ITEMS:	**YES**	**NO**	**N/A**
1.2.1. Are users of SFMIS made aware of Privacy Act of 1974 requirements and responsibilities, the sensitivity of the information entered into DIBRS, and the requirement to report data only to those who have a need-to-know in the performance of official duty? (Para 1.2.7.3.)			
1.2.2. Are all SFMIS modules being utilized? (Para 3.2.4.)			
1.2.3. Are SFMIS users assigned a password? (Para 3.3.1.)			
1.2.4. Is SFMIS data handled as For Official Use Only? (Para 3.3.3.)			
1.2.5. Is the SA utilizing the most current version of Netscape or Internet Explorer browser to ensure proper operation of the system? (Para 4.1.)			
1.2.6. Are measures in place to ensure data displayed on monitors is kept from unauthorized viewing and that privacy data is always protected? (Para 4.2.1.)			
1.2.7. Are SA contacting the Field Assistance Branch (FAB) for assistance on any SFMIS computer problems encountered? (Para 4.3.)			